WE CLAIM:

1. A portable computing device for opening a door, comprising:

a memory, wherein a content of the memory comprises:

a first copy of a shared secret key;

a first standard certificate, wherein the first standard certificate is being used in responding to a challenge of the door; and

means for communicating with the door, wherein the door possesses a second copy of the shared secret key, and wherein the door adapted to validate identicalness of the first and the second copies of the shared secret key, and wherein the door further adapted to issue the challenge to the computing device.

2. The computing device of claim 1, wherein the first standard certificate is having a private key part and the private key part is being encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device.

3. The computing device of claim 2, further comprising a biometric device, wherein the biometric device is capable of generating a second biometric key, wherein the second biometric key belongs to a user of the computing device, and wherein the second biometric key is used to decrypt the private key part of the first standard certificate.

4. A method for secure unlocking of a door based on a shared secret key, comprising the steps of:

providing a portable computing device, wherein the computing device is equipped with a memory, and the memory holds a first copy of the shared secret key and a first standard certificate, wherein the computing device is adapted for performing operations with shared secret keys and standard certificates, and wherein the computing device is also having means for communicating with the door;

communicating by the computing device to the door a device identifier;

issuing a challenge by the door to the computing device, wherein the challenge is issued only on randomly selected occasions;

responding to the challenge by the computing device by demonstrating possession of a private key part of the first standard certificate;

responding by the door with a door identifier and with a message, wherein the message is encrypted with a second copy of the shared secret key, and wherein using the second copy of the shared secret key for encrypting the message resulted from recognizing the device identifier communicated by the computing device;

responding by the computing device with a signal attesting decryption of the message, wherein the message has been decrypted in the computing device by the first copy of the shared secret key, and wherein using the first copy of the shared secret key for decrypting the message resulted from recognizing the door identifier transmitted by the door; and

unlocking the door upon recognizing validity of the signal attesting decryption of the message.

5. The method of claim 4, wherein the device identifier is a hash code of the first standard certificate.

6. The method of claim 4, wherein the door identifier is a simple identifier and it is sent without encryption.

7. The method of claim 4, wherein the door has a second standard certificate, and the door identifier is a hash code of the second standard certificate.

8. The method of claim 4, wherein the shared secret key is generated by the door and communicated with the computing device in private using a public key part of the first standard certificate.

9. The method of claim 4, wherein the private key part of the first standard certificate is encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device, and wherein the computing device is provided with a biometric device, and wherein the step of responding to the challenge further comprise the steps of:

taking a biometric reading of a user of the computing device;

generating a second biometric key using the biometric reading; and

decrypting the encrypted private key part of the first standard certificate using the second biometric key, whereby if the first and second biometric keys are identical the decrypting using the second biometric key is successful, and the challenge can be successfully responded.

10. A security system for controlling access, comprising a first plurality of doors and a second plurality of portable computing devices for opening doors, each computing device equipped with a memory, wherein any one of the computing devices holds in its memory a unique first standard certificate, and wherein the any one computing device further holds in its memory door identifiers for all those doors out of the first plurality of doors that the any one computing device is permitted to open, and wherein each of the door identifier is uniquely linked to a first copy of a shared secret key, wherein any one of the doors possesses a matching information for each one of those computing devices out of the second plurality of computing devices that are permitted to open the any one door, wherein the matching information comprises a device identifier, wherein the device identifier is linked to a public key part of the unique first standard certificate and to a second copy of the shared secret key, and wherein the first plurality of doors and the second plurality of computing devices have means for communicating between any device and any door, and wherein the any one door is adapted to recognize the device

identifier, and further adapted to use the matching information to validate identicalness of the first and the second copies of the shared secret key, and to issue a challenge to the unique first standard certificate using the public key part of the unique first standard certificate.

11. The security system of claim 10, wherein the device identifier is a hash code of the unique first standard certificate.

12. The security system of claim 10, wherein the door identifier is a simple identifier and it is communicated without encryption.

13. The security system of claim 10, wherein the any one door further possesses a unique second standard certificate.

14. The security system of claim 13, wherein the door identifier is a hash code of the unique second standard certificate.

15. The security system of claim 10, wherein the challenge is issued on randomly selected occasions.

16. The security system of claim 10, wherein the unique first standard certificate is having a private key part and the private key part is being encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device.

17. The security system of claim 16, wherein the any one computing device is further comprising a biometric device, wherein the biometric device is capable of generating a second biometric key, wherein the second biometric key belongs to a user of the any one computing device, and wherein the second biometric key is used to decrypt the private key part of the unique first standard certificate.

18. The security system of claim 10, wherein the challenge by the any one door is successfully responded by demonstrating possession of a private key part of the unique first standard certificate.

19. The security system of claim 10, wherein the any one door is further adapted to generate a shared secret key and communicate the shared key in private by using the public key part of the unique first standard certificate.

20. A computer data signal embodied in a carrier wave encoding a computer program of instructions for executing a computer process performing the steps for secure unlocking of a door based on a shared secret key, as recited in the steps of:

communicating by a computing device to the door a device identifier;

issuing a challenge by the door to the computing device, wherein the challenge is issued only on randomly selected occasions;

responding to the challenge by the computing device by demonstrating possession of a private key part of a first standard certificate;

responding by the door with a door identifier and with a message, wherein the message is encrypted with a second copy of the shared secret key, and wherein using the second copy of the shared secret key for encrypting the message resulted from recognizing the device identifier communicated by the computing device;

responding by the computing device with a signal attesting decryption of the message, wherein the message has been decrypted in the computing device by the first copy of the shared secret key, and wherein using the first copy of the shared secret key for decrypting the message resulted from recognizing the door identifier transmitted by the door; and

unlocking the door upon recognizing validity of the signal attesting decryption of the message.